HyperAgent Custody Architecture

Security Brief · January 2026

Zero-Custody Design

HyperAgent operates on a trustless, non-custodial architecture. Your private keys never leave your control. We only request trade-execution API permissions - withdrawal rights are never requested or stored.

Three-Plane Architecture

Plane	Responsibility	Custody
Client Signer	Private key storage, signature generation	User-controlled (laptop/HSM/MPC)
BrainCenter	Strategy execution, risk validation, monitoring	No keys - only signed payloads
Hyperliquid	Order matching, position management	Exchange-controlled

17 Active Safety Gates

Edge validation • Spread protection • Funding rate gate • Trend filter • Volatility regime • Orderbook depth • OI utilization • Solvency check • Regime gate • Neutral bias gate • Post-restart cooldown • Conviction floor • Liquidity validation • Position limits • Leverage caps • Circuit breaker • Watchdog override

Infrastructure Hardening

• **Circuit Breaker**: Max 10 restarts/hour prevents crash loops with auto-disable

• **Safety Watchdog**: Independent process monitors positions 24/7 with stop-loss enforcement

• **OOM Protection**: Memory priority scoring prevents kernel kills during high load

• **Telegram Alerts**: Real-time notifications for regime changes, errors, and critical events

Audit Trail

Every decision is logged with SHA-256 hashes. ErrorWatcher auto-opens support tickets with full context. Redis persistence ensures state survives restarts. All logs are retained for compliance review.

Document Hash: SHA-256 verification available on request
Generated: 2026-01-04 02:44:16 UTC